

FIG. 1

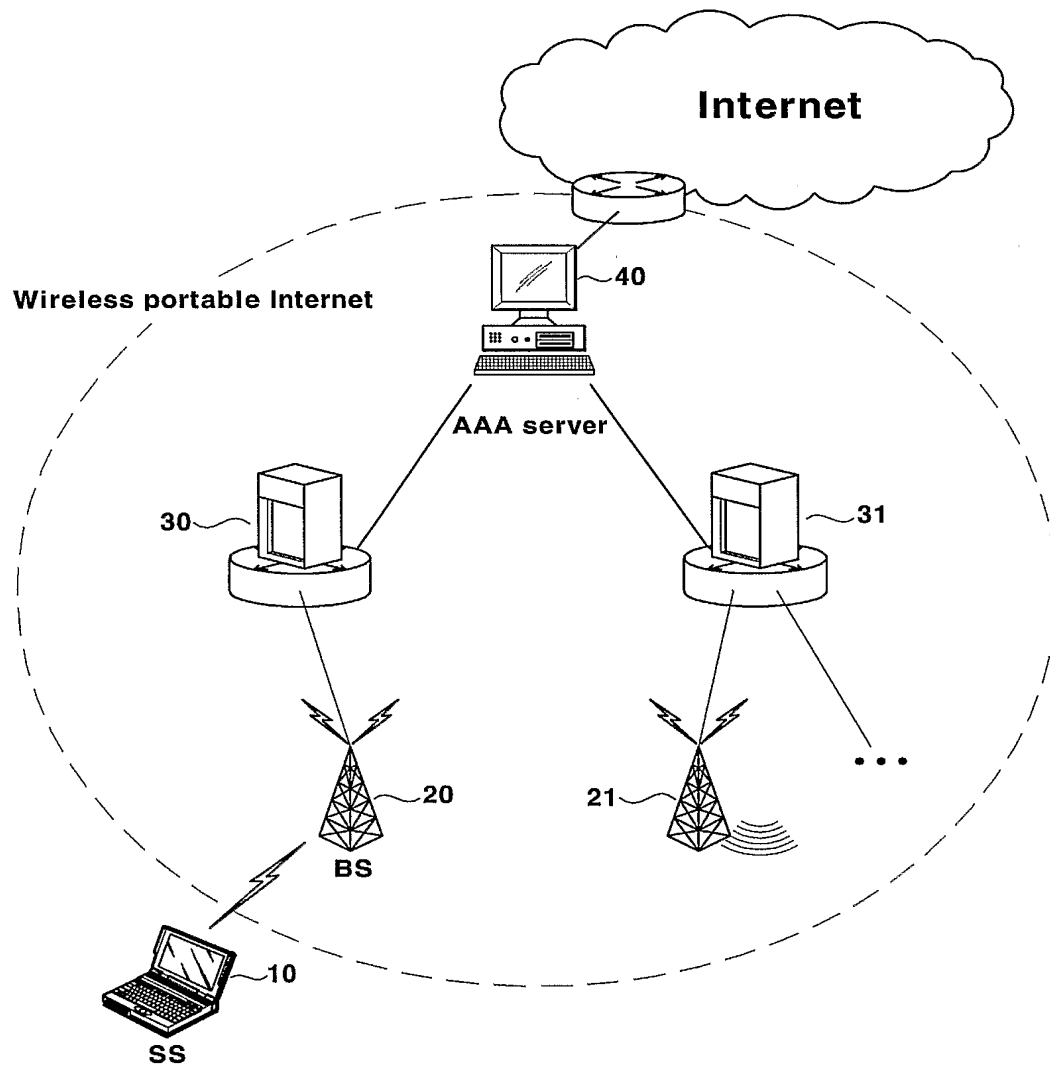


FIG. 2

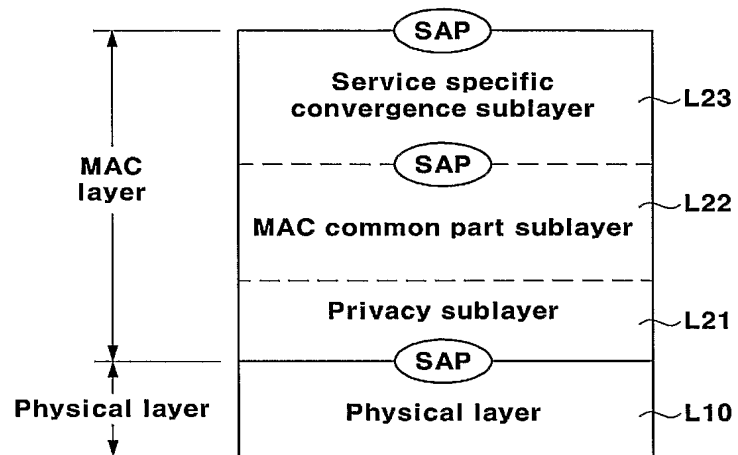


FIG. 3

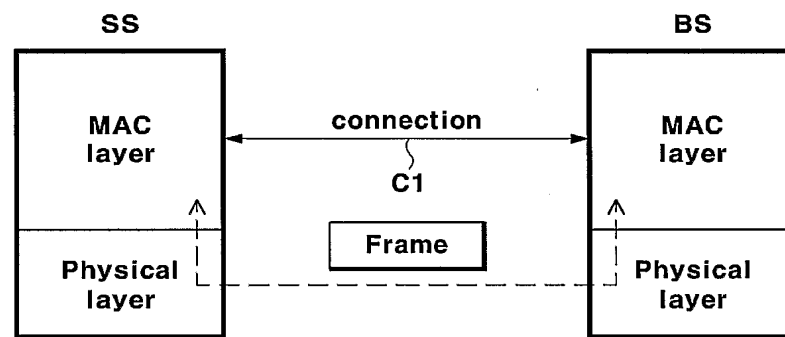


FIG. 4

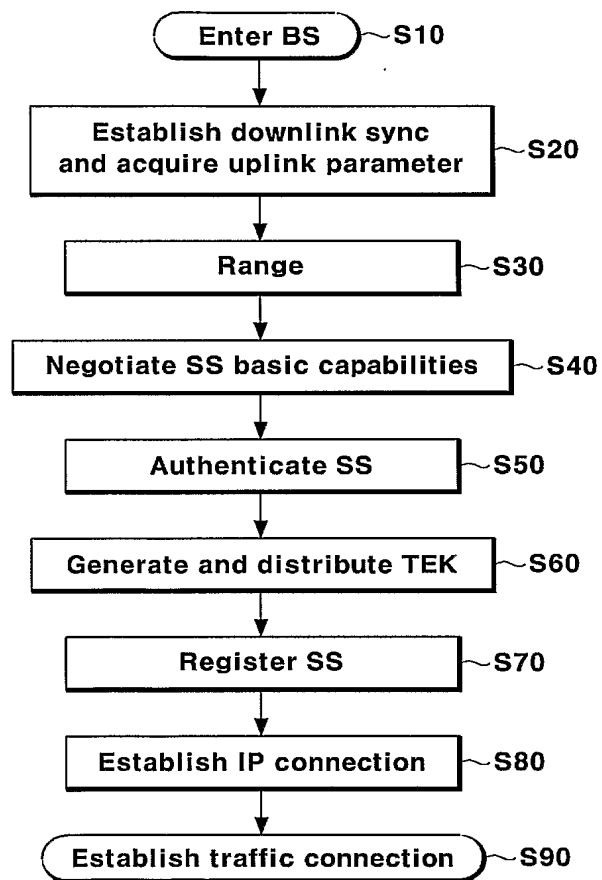


FIG. 5

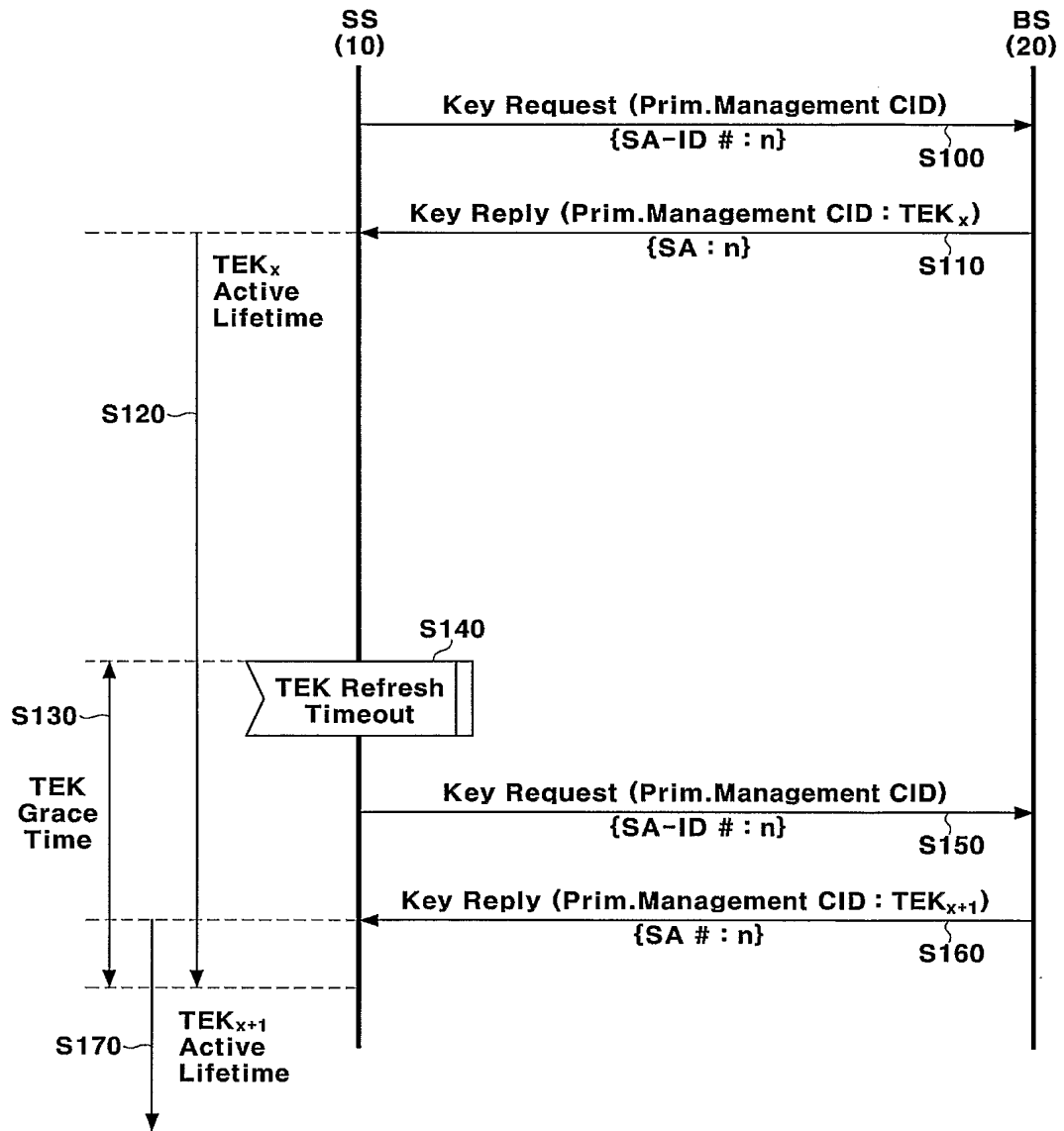


FIG. 6

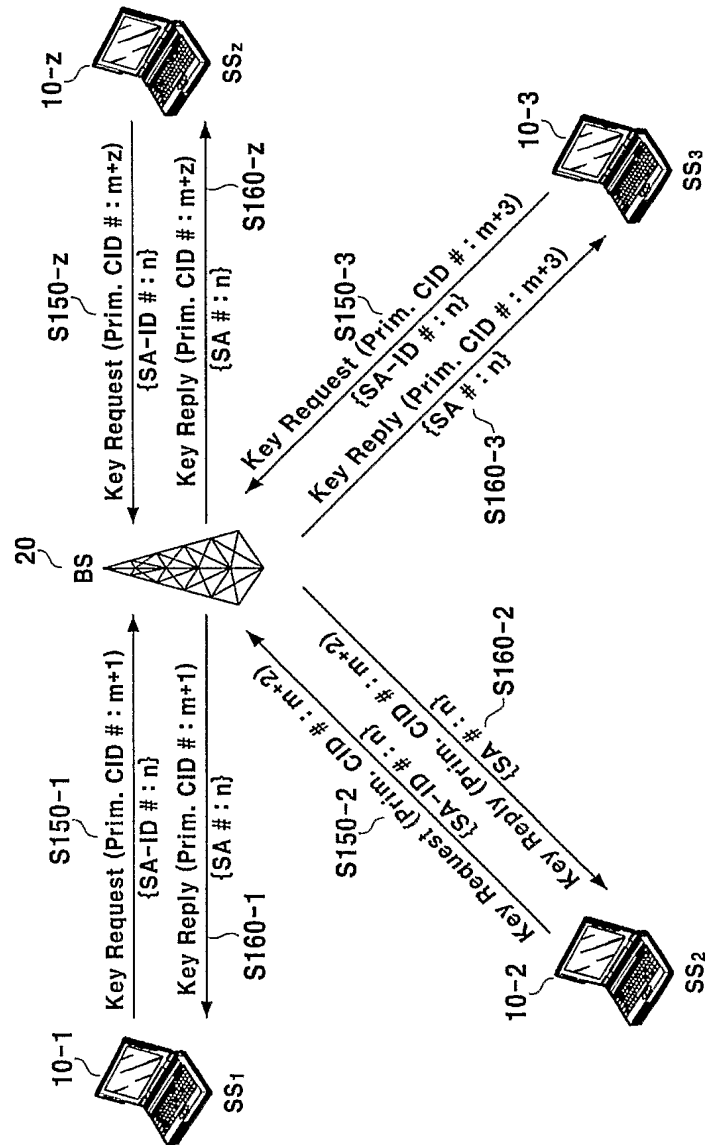


FIG. 7

System	Name	Description	Minimum value	Default value	Maximum value
BS	M&B TEK Grace Time	Time prior to TEK (for the multicast and broadcast traffic service) expiration. BS begins rekeying. This time is longer than the TEK Grace Time.	Vendor-specific value	Vendor-specific value	Vendor-specific value

FIG. 8

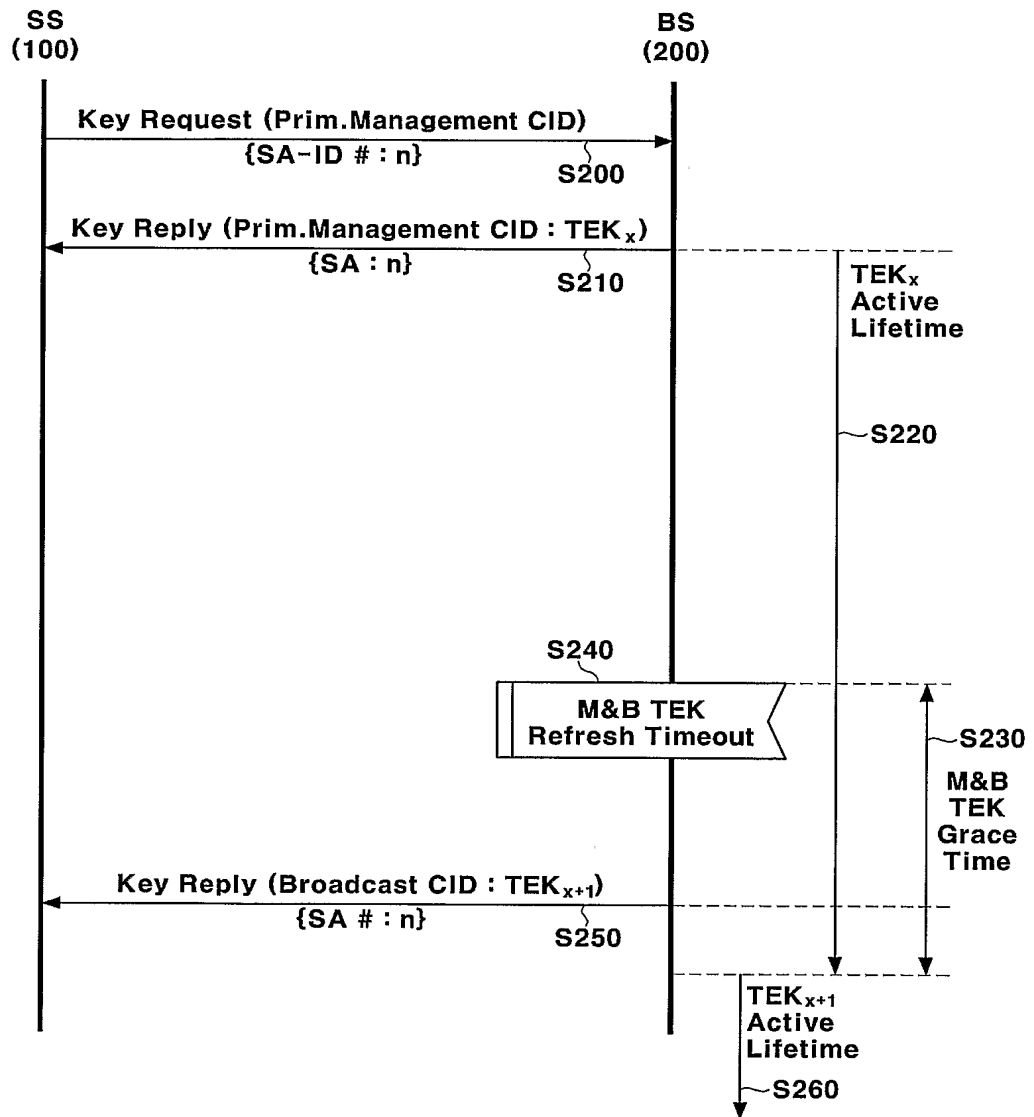


FIG. 9

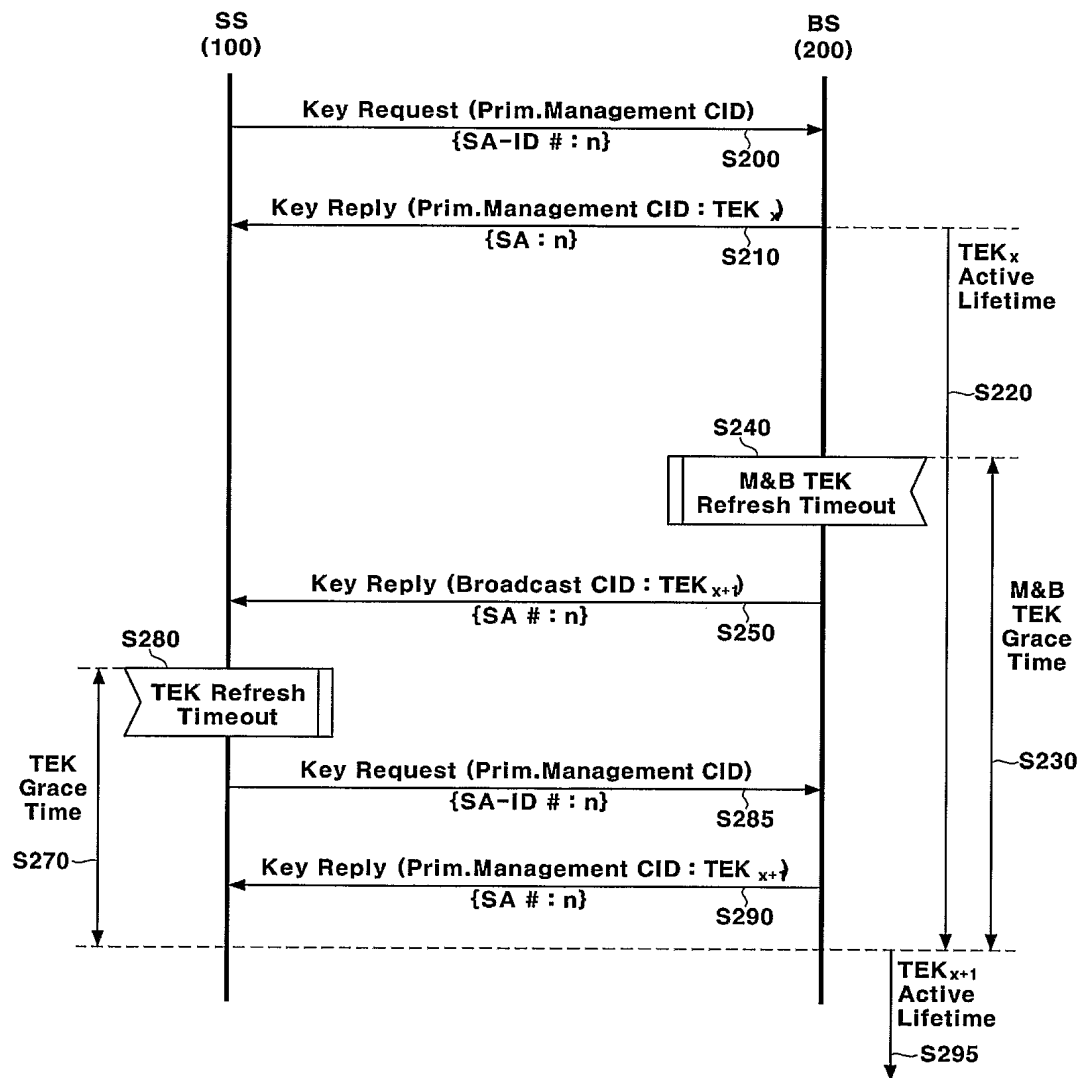


FIG. 10

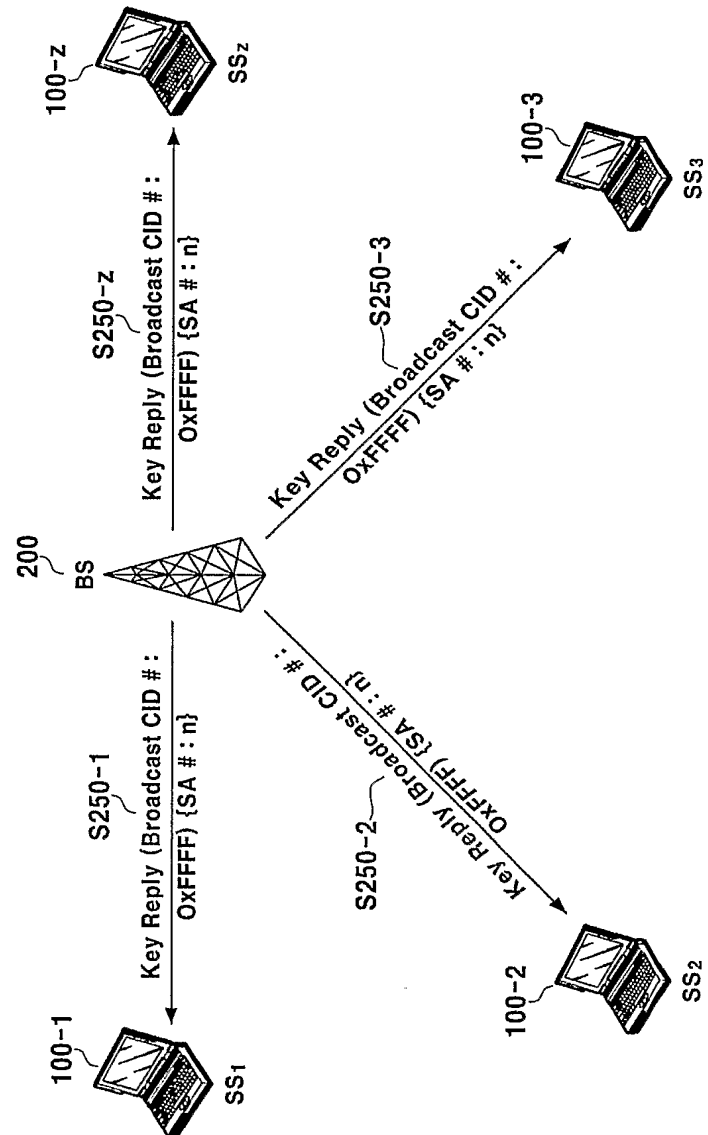


FIG. 11

CID(MAC Header)	Key to encrypt the TEK
Primary Management CID	KEK(Derived from the AK)
Broadcast CID	Old distributed TEK

FIG. 12

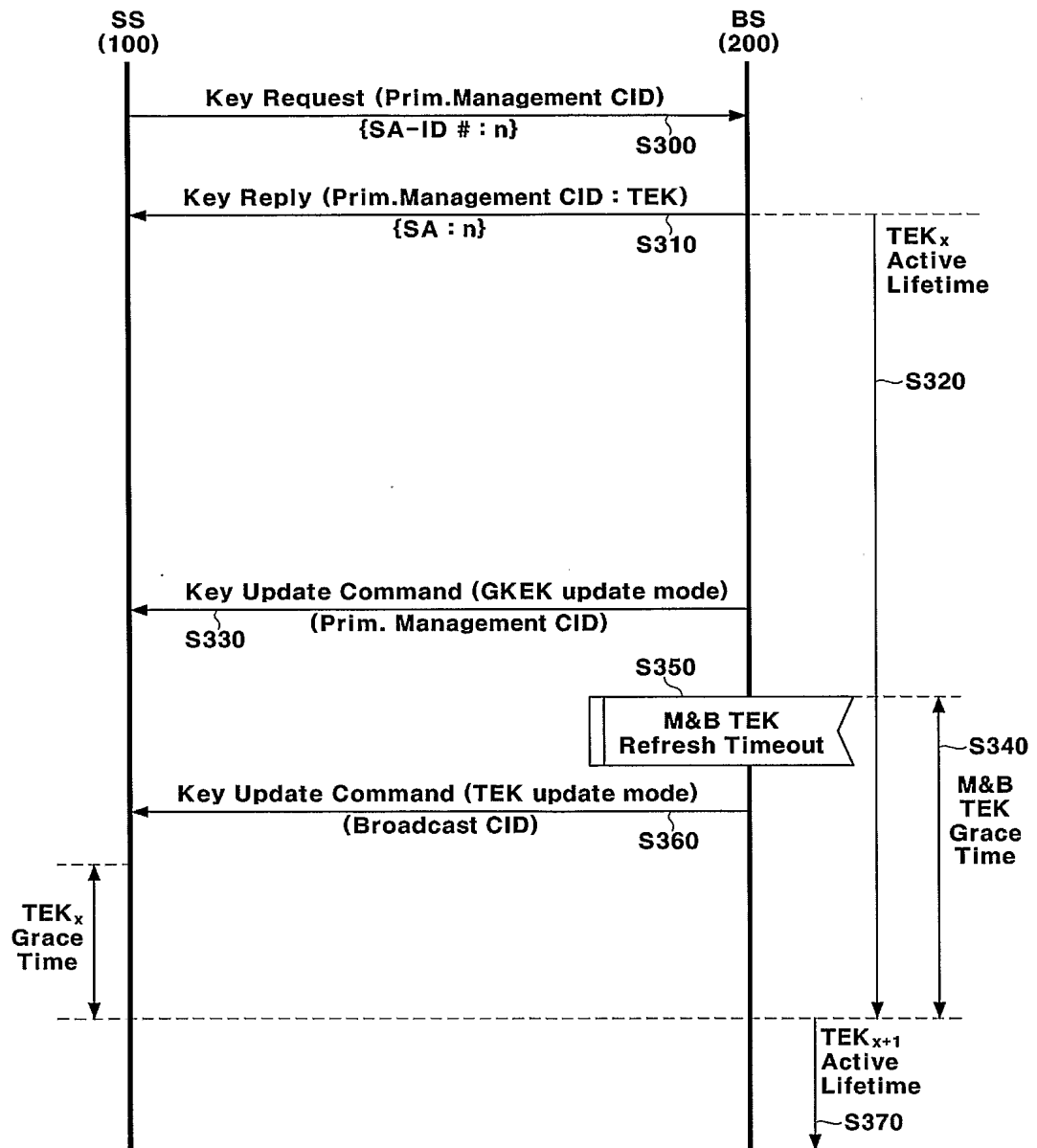


FIG. 13

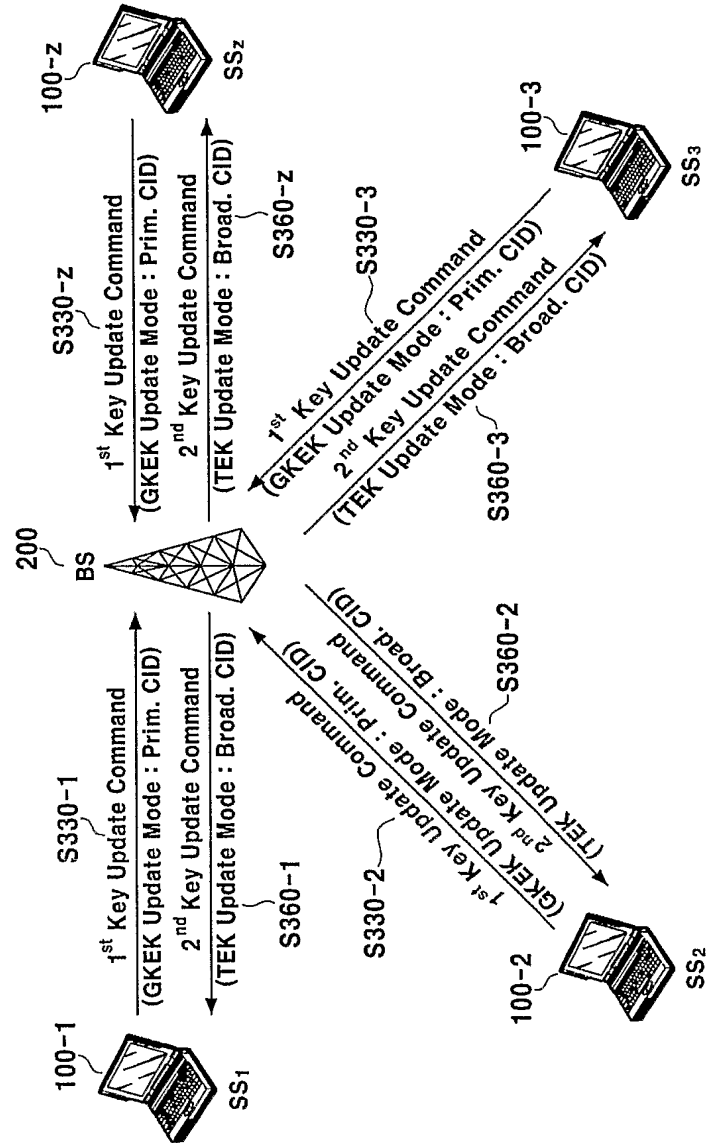


FIG. 14

Attributes	Contents
Key-Sequence-Number	Authorization Key sequence number
SAID	Security Association ID
TEK-Parameters	"Older" generation of key parameters relevant to SAID
TEK-Parameters	"Newer" generation of key parameters relevant to SAID
HMAC-Digest	Keyed SHA message digest

FIG. 15

Attributes	Contents
GKEK	GKEK, encrypted with the AK
TEK	TEK, encrypted with the GKEK (Multicast or Broadcast Service) or encrypted with the KEK (Unicast Service)
Key-Lifetime	TEK Remaining Lifetime
Key-Sequence-Number	TEK Sequence Number
CBC-IV	Cipher Block Chaining (CBC) Initialization Vector

FIG. 16

Attributes	Contents	1 st Message (Primary)	2 nd Message (Broadcast)
Key-Sequence-Number	Authorization key sequence number	○	○
SAID	Security Association ID	○	○
Key Push Modes	Usage code of Key Update Command message	○	○
Key Push Counter	Counter one greater than that of older generation for reply attack	○	○
TEK-Parameters	"Newer" generation of key parameters relevant to SAID		
> GKEK	GKEK, encrypted with the AK	○	×
> TEK	TEK, encrypted with the GKEK (Multicast or Broadcast Service)	×	○
> Key-Lifetime	TEK Remaining Lifetime	×	○
> Key-Sequence-Number	TEK Sequence Number	○	○
> CBS-IV	Cipher Block Chaining (CBC) Initialization Vector	×	○
HMAC-Digest	Keyed SHA message digest	○	○

FIG. 17

Type	Length	Value
30	1	0, GKEK update mode (1 st Message) 1, TEK update mode (2 nd Message) 2-225, reserved

FIG. 18

Key push modes	Input Key
GKEK update mode	AK
TEK update mode	GKEK

FIG. 19

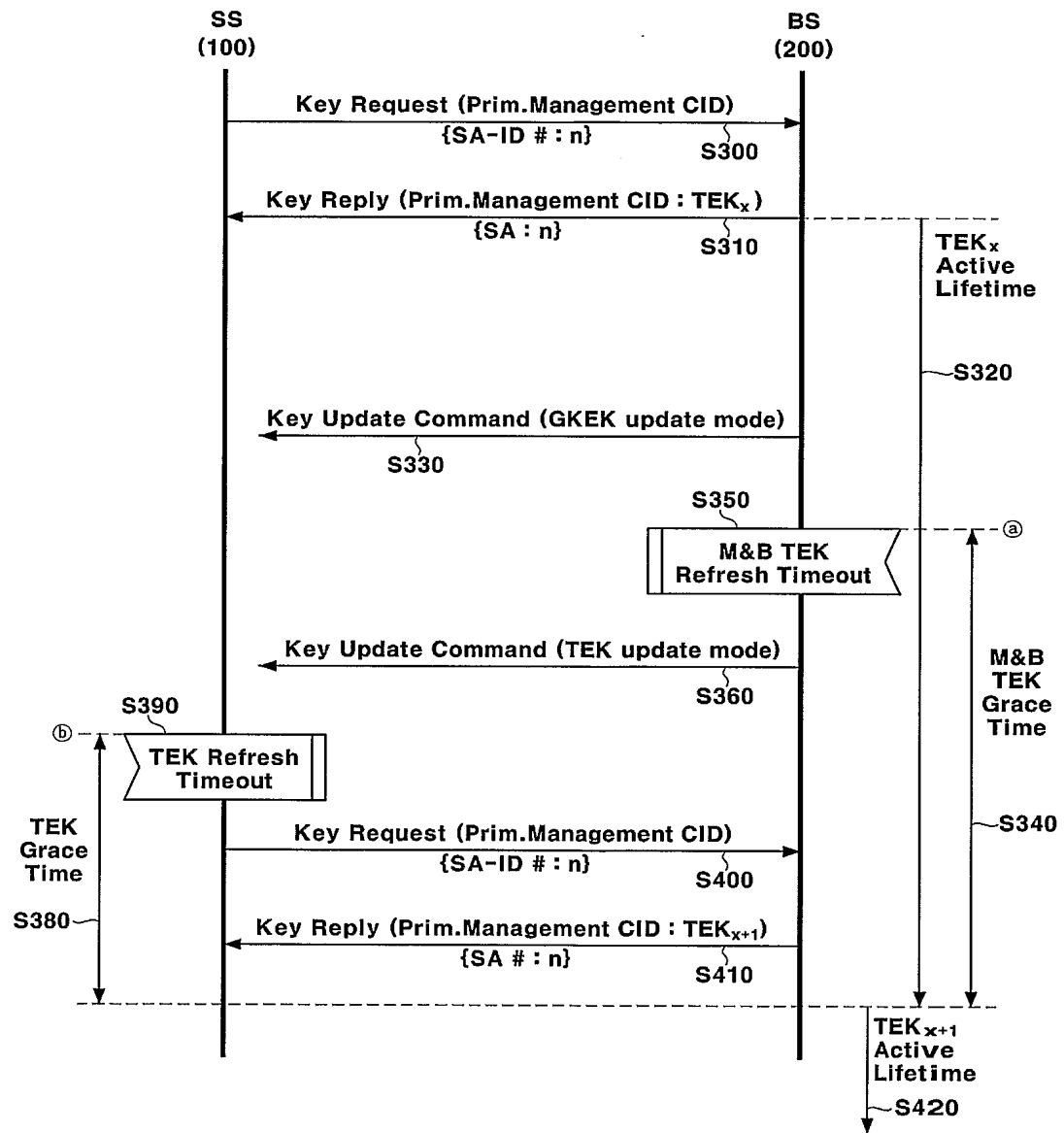


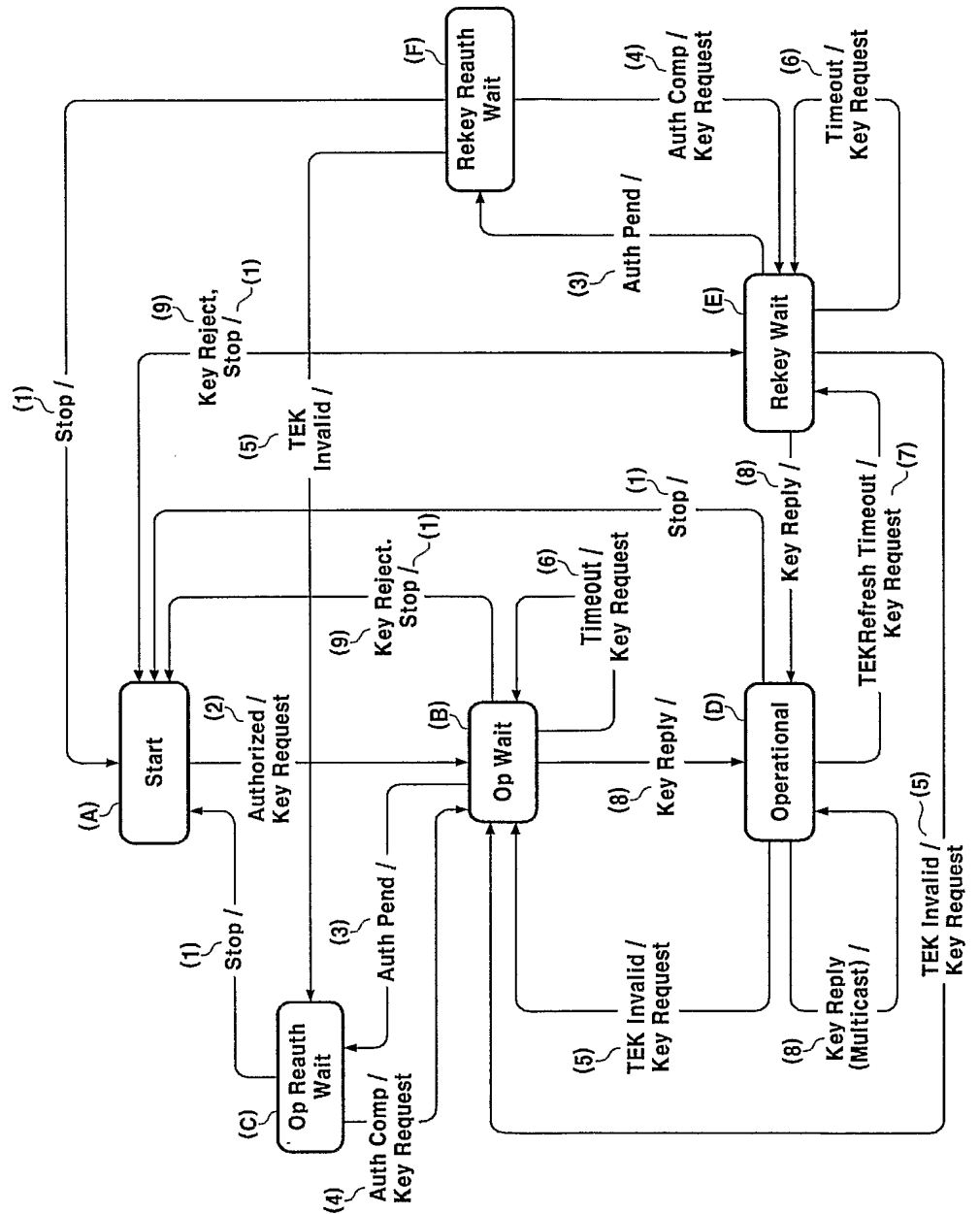
FIG. 20

Situation	Transferred TEK-parameter information
Initial TEK response (before ③)	TEK-parameters _C
Initial TEK response (after ③)	TEK-parameters _C & TEK-parameters _N
Initial update response (after ④)	TEK-parameters _N

C : Current generation of key parameters relevant to SAID

N : Next generation of key parameters relevant to SAID

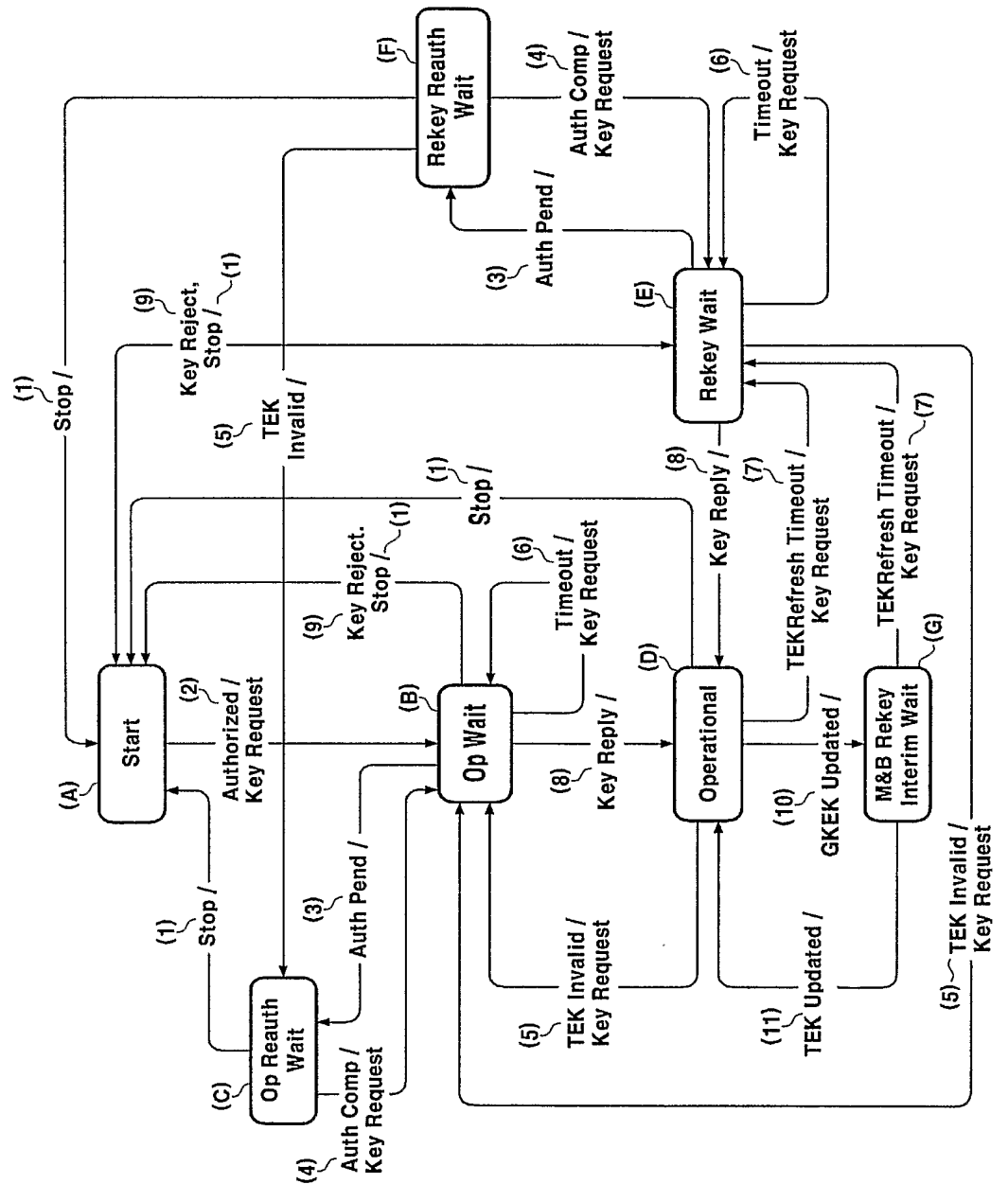
FIG. 21



[Fig. 22]

State Event or Rcvd Message	(A) Start	(B) Op Wait	(C) Op Reauth Wait	(D) Op	(E) Rekey Wait	(F) Rekey Reauth Wait
(1) Stop		Start	Start	Start	Start	Start
(2) Authorized	Op Wait					
(3) Auth Pend		Op Reauth Wait			Rekey Reauth Wait	
(4) Auth Comp			Op Wait			Rekey Wait
(5) TEK Invalid				Op Wait	Op Wait	Op Reauth Wait
(6) Timeout		Op Wait			Rekey Wait	
(7) TEK Refresh Timeout				Rekey Wait		
(8) Key Reply		Operational		Operational	Operational	
(9) Key Reject		Start			Start	

FIG. 23



[Fig. 24]

State Event or Rcvd Message	(A) Start	(B) Op Wait	(C) Op Reauth Wait	(D) Op	(E) Rekey Wait	(F) Rekey Reauth Wait	(G) M&B rekey Interim Wait
(1) Stop		Start	Start	Start	Start	Start	
(2) Authorized	Op Wait						
(3) Auth Pend		Op Reauth Wait			Rekey Reauth Wait		
(4) Auth Comp			Op Wait			Rekey Wait	
(5) TEK Invalid				Op Wait	Op Wait	Op Reauth Wait	
(6) Timeout		Op Wait			Rekey Wait		
(7) TEK Refresh Timeout				Rekey Wait			Rekey Wait
(8) Key Reply		Operational			Operational		
(9) Key Reject		Start			Start		
(10) GKEK Updated				Rekey Wait			
(11) TEK Updated							Operational